machine. As noted above, some preferred embodiments of the present invention include parallel, digital interfaces for high-speed data transfer. However, even the serial devices may have electrical interface requirements that differ from the "standard" EIA RS232 serial interfaces provided by general-purpose computers. These interfaces may include EIA RS485, EIA RS422, Fiber Optic Serial, Optically Coupled Serial Interfaces, current loop style serial interfaces, etc. In addition, to conserve serial interfaces internally in the slot machine, serial devices may be connected in a shared, daisy-chain fashion where multiple peripheral devices are connected to a single serial channel.

[**0230**] IGT Gaming machines may alternatively be treated as peripheral devices to a casino communication controller and connected in a shared daisy chain fashion to a single serial interface. In both cases, the peripheral devices are preferably assigned device addresses. If so, the serial controller circuitry must implement a method to generate or detect unique device addresses. General-purpose computer serial ports are not able to do this.

[**0231**] Security monitoring circuits detect intrusion into an IGT gaming machine by monitoring security switches attached to access doors in the slot machine cabinet. Preferably, access violations result in suspension of game play and can trigger additional security operations to preserve the current state of game play. These circuits also function when power is off by use of a battery backup. In power-off operation, these circuits continue to monitor the access doors of the slot machine. When power is restored, the gaming machine can determine whether any security violations occurred while power was off, e.g., via software for reading status registers. This can trigger event log entries and further data authentication operations by the slot machine software.

[**0232**] Trusted memory devices are preferably included in an IGT gaming machine computer to ensure the authenticity of the software that may be stored on less secure memory subsystems, such as mass storage devices. Trusted memory devices and controlling circuitry are typically designed to not allow modification of the code and data stored in the memory device while the memory device is installed in the slot machine. The code and data stored in these devices may include authentication algorithms, random number generators, authentication keys, operating system kernels, etc. The purpose of these trusted memory devices is to provide gaming regulatory authorities a root trusted authority within the computing environment of the slot machine that can be tracked and verified as original. This may be accomplished via removal of the trusted memory device from the slot machine computer and verification of the trusted memory device contents in a separate third party verification device. Once the trusted memory device is verified as authentic, and based on the approval of the verification algorithms contained in the trusted device, the gaming machine is allowed to verify the authenticity of additional code and data that may be located in the gaming computer assembly, such as code and data stored on hard disk drives.

[**0233**] Mass storage devices used in a general-purpose computer typically allow code and data to be read from and written to the mass storage device. In a gaming machine environment, modification of the gaming code stored on a mass storage device is strictly controlled and would only be allowed under specific maintenance type events with electronic and physical enablers required. Though this level of security could be provided by software, IGT gaming computers that include mass storage devices preferably include hardware level mass storage data protection circuitry that operates at the circuit level to monitor attempts to modify data on the mass storage device and will generate both software and hardware error triggers should a data modification be attempted without the proper electronic and physical enablers being present.

[**0234**] Gaming machines used for Class III games generally include software and/or hardware for generating random numbers. However, gaming machines used for Class II games may or may not have RNG capabilities. In some machines used for Class II games, RNG capability may be disabled.

[**0235**] **FIG. 26** illustrates an example of a network device that may be configured as a game server for implementing some methods of the present invention. Network device **2660** includes a master central processing unit (CPU) **2662**, interfaces **2668**, and a bus **2667** (e.g., a PCI bus). Generally, interfaces **2668** include ports **2669** appropriate for communication with the appropriate media. In some embodiments, one or more of interfaces **2668** includes at least one independent processor and, in some instances, volatile RAM. The independent processors may be, for example, ASICs or any other appropriate processors. According to some such embodiments, these independent processors perform at least some of the functions of the logic described herein. In some embodiments, one or more of interfaces **2668** control such communications-intensive tasks as media control and management. By providing separate processors for the communications-intensive tasks, interfaces **2668** allow the master microprocessor **2662** efficiently to perform other functions such as routing computations, network diagnostics, security functions, etc.

[**0236**] The interfaces **2668** are typically provided as interface cards (sometimes referred to as "linecards"). Generally, interfaces **2668** control the sending and receiving of data packets over the network and sometimes support other peripherals used with the network device **2660**. Among the interfaces that may be provided are FC interfaces, Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided, such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces, ASI interfaces, DHEI interfaces and the like.

[**0237**] When acting under the control of appropriate software or firmware, in some implementations of the invention CPU **2662** may be responsible for implementing specific functions associated with the functions of a desired network device. According to some embodiments, CPU **2662** accomplishes all these functions under the control of software including an operating system and any appropriate applications software.

[**0238**] CPU **2662** may include one or more processors **2663** such as a processor from the Motorola family of microprocessors or the MIPS family of microprocessors. In an alternative embodiment, processor **2663** is specially designed hardware for controlling the operations of network device **2660**. In a specific embodiment, a memory **2661**